أستكشاف أخطاء حزم FTD وإصلاحها (tcp-not-syn) عند "؛التطبيق المحسن واكتشاف URL&cut؛ تم تمكينها على الواجهات الداخلية مع تدفق حركة المرور غير المتماثل

المحتويات

مسألة

تقوم أجهزة الدفاع عن تهديد جدار الحماية (FTD) التي تم تكوينها باستخدام مجموعات الواجهة (ASP) المضمنة بإسقاط حركة مرور إرجاع TCP باستخدام سبب إسقاط مسار الأمان السريع tcp-not-syn. يحدث هذا مباشرة بعد تمكين ميزة اكتشاف هوية خادم TLS (TSID) - وخاصة خيار "التطبيق المحسن واكتشاف عنوان URL". في إصدارات مركز إدارة جدار الحماية (FMC) الأقدم، يسمى الخيار "الكشف المبكر عن التطبيقات وتصنيف URL". يتم إسقاط حزم TCP syn-ack التي تم اعتراضها، الأصلي SYN وجيه أعاد توجيه نفسه الذي FTD جهاز بواسطة إرجاع مسار على ack إنشاء جلسات عمل TCP.

يظهر الإصدار كحالات فشل اتصال TCP واسعة النطاق ولا يقتصر على حركة مرور TLS. يتم ملاحظة هذه الأعراض عند تمكين الميزة:

- يتم إسقاط حزم TCP syn-ack على مسار الإرجاع باستخدام سبب إسقاط ASP tcp-not-syn.
- لا تظهر جلسات عمل TCP الجديدة في جدول اتصال FTD.
- تتراكم عدادات إسقاط ASP المرتفعة بسرعة، كما هو موضح من خلال هذا الإخراج المضمن بعد 10 دقائق تقريبا من تمكين الميزة:

```
<#root>

device#

show asp drop

Frame drop:
                                                                1
  Flow is denied by configured rule (acl-drop)
```

```
First TCP packet not SYN (tcp-not-syn)                                  34802

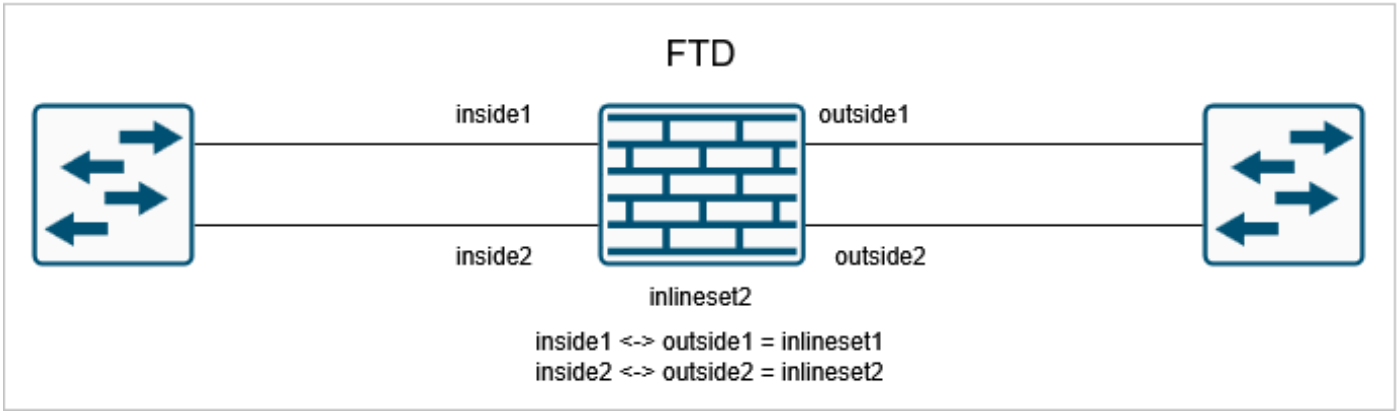
TCP RST/FIN out of order (tcp-rstfin-ooo)                                   4
Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                             995
Dropped pending packets in a closed socket (np-socket-closed)               3
TCP Proxy probe reset injected (tcp-proxy-probe-rst-injected)               1
TCP Proxy probe receive drop (tcp-proxy-probe-tcp-probe-drop)               1
Blocked or blacklisted by the reputation preprocessor (reputation)          1

                                Last clearing: 16:50:21 CEST Oct 24 2026 by enable_1
```

البيئة

- النظام الأساسي: Cisco Firepower 4115. كما يمكن أن تتأثر منصات العمل الأخرى.
- إصدار برنامج FTD: 7-6-4 ويمكن أن تتأثر أيضا إصدارات البرامج الأخرى.
- إصدار برنامج FMC: 10.1.0. قد تتأثر أيضا إصدارات البرامج الأخرى.
- FTD مع مجموعات الواجهة المضمنة.
- يحتوي FTD على إثنين من أزواج الواجهة المضمنة على الأقل: inlineset1 و inlineset2 (أو أن هناك إثنان FTDs مختلف مع كل واحد مجموعة أسطر واحدة).
- تدفق حركة المرور غير المتماثل الموجود في البيئة: يقوم TCP syn بترحيل عبر الواجهة الخارجية1 بينما ترجع TCP SYN-ACK المطابقة عبر الواجهة outside2 على جهاز FTD نفسه.
- يتم تمكين ميزة TSID على FTD.

المخطط



رارق

إن الحل الموصى به لإيقاف إسقاط اتصال TCP-not-syn واستعادته من خلال واجهات FTD .TSID لداخل URL "التطبيق المحسن واكتشاف عنوان" الخيار تعطيل هو وهذا يسمح المضمنة وهو أمر ضروري لاستيعاب بتجاوز حالة TCP بأن يظل نشطا على مجموعات الواجهة الداخلية، وهو تدفقات حركة المرور غير المتماثلة في البيئة.

تعطيل "التطبيق المحسن واكتشاف عنوان URL" في FMC

انتقل إلى: سياسات > التحكم في الوصول > [سياسة التحكم في الوصول الخاصة بك] > متقدم > اكتشاف هوية خادم TLS. قم بإلغاء تحديد أو تعطيل خانة الاختيار "التطبيق المحسن وكشف URL"، ثم قم بنشر النهج إلى أجهزة FTD المتأثرة.

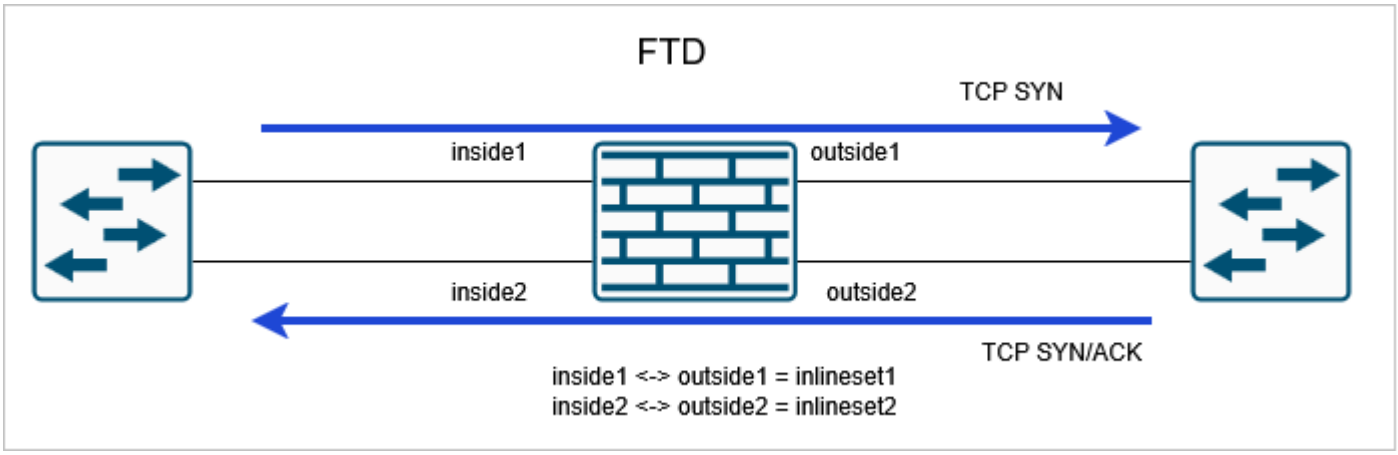
بعد تعطيل الميزة، تظهر جلسات عمل جديدة في جدول الاتصال، مما يؤكد أن اتصالات TCP تقوم بإكمال المصافحة الثلاثية بنجاح.

ملاحظة: مع تعطيل TSID، لم يعد بإمكان FTD رؤية شهادة الخادم في جلسات عمل TLS لتطابق قواعد التطبيق وعنوان URL حركة مرور البيانات بشكل أقل دقة على حركة المرور المشفرة. 1.3.

السبب

يتمثل السبب الجذري لعمليات إسقاط TCP-not-syn في عدم توافق بين ميزة TLS Server Identity Discovery وتجاوز حالة TCP على مجموعات الواجهة المضمنة في FTD.

بشكل افتراضي، يتم تمكين تجاوز حالة TCP لحركة المرور عبر الواجهات الداخلية على FTD. تم تصميم تجاوز حالة TCP للسماح بحركة المرور غير المتماثلة - حيث يمكن للمسارات المختلفة - للتمرير دون إجتياز واجهات مختلفة أو حتى أجهزة مختلفة للاتصال TCP الأمامية والخلفية. هذا سلوك ضروري في البيئات التي يكون فيها عدم تماثل التوجيه موجود: FTD بفرض تعقب صارم لحالة TCP. يقوم

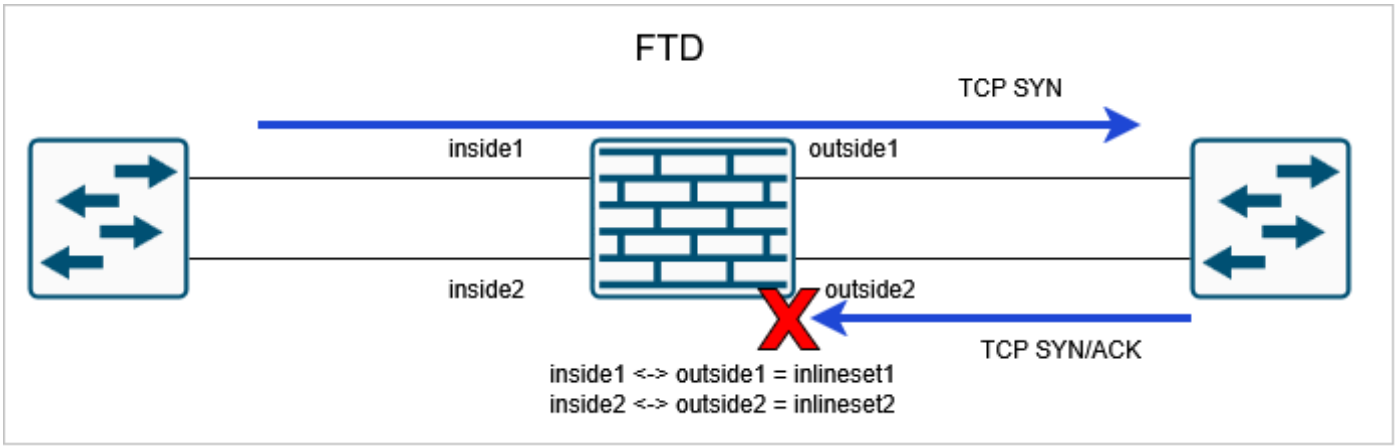


تدفق TCP غير المتماثل من خلال مجموعات أسطر FTD المضمنة عند تعطيل TSID.

ومع ذلك، عند تمكين أي من هذه الميزات، يتجاوز نظام FTD تجاوز حالة TCP ويبدأ في إجراء فحوصات حالة TCP بالكامل على حركة مرور الواجهة المضمنة:

- خيار "التطبيق المحسن واكتشاف عنوان URL" تحت اكتشاف هوية خادم TLS.
- أي نهج فك تشفير TLS/SSL نشط.

بمجرد فرض فحوصات حالة TCP، يقوم FTD بتعقب تسلسل مصافحة TCP بالكامل. في البيئات ذات التوجيه غير المتماثل — حيث، على سبيل المثال، تخرج حزمة TCP syn عبر الواجهة الخارجية1 ولكن ترجع TCP SYN-ACK المقابلة عبر الواجهة الخارجية على الجهاز نفسه — لا يتعرف FTD على SYN-ACK على أنه ينتمي إلى جلسة TCP المعروفة والمتعقبة. نظرا لأن SYN-ACK يصل إلى واجهة مختلفة عن ما هو متوقع ولم يتم مشاهدة أي اتصال غير معروف SYN حزمة، فإن FTD يصنفه على نظام مقابل على تلك الواجهة، ويطلقه باستخدام سبب إسقاط ASP tcp-not-syn.



تدفق TCP غير المتماثل من خلال مجموعات الأسطر الداخلية ل FTD عند تمكين TSID.

المحتوى ذي الصلة

- [ةيوه فاشكتسا قافوتم مدع :قئاثولا — Cisco CSCwp84746 نم ءاطخألا حيحصت فرعم رطسألا ةعومجم تاهاوو على TCP ةلاح زواجت عم TLS مداخ](#)
- [TLS مداخ فرعم فاشكتسا ىطخت :Doc — Cisco CSCwx42897 نم ءاطخألا حيحصت فرعم TCP (tcp-not-syn) رورم ةكرح طاقسإ في ببستي امم ،رطسألا ةعومجم تاهاوو على TCP ةلاح زواجت](#)
- [فاشكتسا" نيكمت دنع اريذحت فضأ — Cisco CSCwx42901 نم ءاطخألا حيحصت فرعم ةعومجم تاهاوو على TCP ةلاح زواجت زجعي هنأ (TSID) "URL في تانايبلا رقم و ةيطيقلا طوطخلا لخادلا](#)
- [(TLS مداخ ةيوه فاشكتسا ديقي نمضتي) TCP ةلاح زواجت لتاشادرا — Cisco قئاثو](#)
- [ةيلخادلا طوطخلا تاعومجم ربع ةلثامتملا ريغ رورملا ةكرح - ةلاح ةسارد](#)
- [يف اهالصاو ءاطخألا فاشكتسأ تاعومجم ءاشنإ ةيفيك — Cisco نم ةينقتلا ةظحالم FMC و FTD جمانرب](#)
- [Cisco نم تالينزلاو ينفلا معدلا](#)

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).